Task 1: Introduction to Network Security Basics

Nicholas Massei

Cybersecurity Intern

Redynox

July 10, 2025

Introduction

In this task, I focused on understanding core network security principles and implementing essential defensive measures in a virtual lab environment. I began by researching the common network threats, including viruses, worms, trojans, and phishing attacks. I then transitioned into setting up and securing a basic network using VirtualBox – with 2 VMs – and my home router. I planned for these exercises to give me hands-on experience with both network defense in theory, and real-world application.

Network Threats

- **Virus**: A virus is malicious code that can attach itself to a legitimate program or file that spreads when the infected item is run or shared. Simply put, viruses can damage files, corrupt systems, and slow down performance.
- **Worm**: A worm is a standalone program that can replicate and spread across networks without user action. Unlike a virus, it doesn't need to attach to a file. Also, worms can often consume bandwidth or overload systems.
- **Trojan Horse**: A trojan is another type of malicious program that relies on pretending to be harmless or useful software. Once a trojan is installed, it can open a back door for attackers, steal sensitive data, or act as a Remote Access Trojan (RAT) to give full remote access of the system to the attacker.
- **Phishing**: Phishing is a common technique that tricks users through emails, websites, or messages into giving away sensitive information such as user credentials or credit card numbers. Attackers often impersonate trusted entities to seem convincing as well. Phishing attacks can range from broad, generic campaigns, to highly targeted attacks that are carefully researched and personalized, such as spear phishing.

Security Concepts

- **Firewalls**: Block/allow traffic based on rules (Windows Defender Firewall).
- **Encryption**: Secures data in transit (such as HTTPS or WPA2/WPA3).
- **Secure Configs**: Changing default router/admin passwords, disabling unused ports, and others.

Reference

National Institute of Standards and Technology. *Computer Security Resource Center Glossary*. U.S. Department of Commerce. https://csrc.nist.gov/glossary

Set up a simple network enviornment

Set up using VirtualBox – 2 virtual machines (Windows 10 & Ubuntu)

Enabled and configured basic firewall on Windows machine using Windows Defender Firewall

Set up other basic security configurations and network encryption by accessing my router's configuration page by entering the default gateway IP address into my web browser (gateway located by utilizing "ipconfig" in powershell). From there, I navigated to the wireless security settings and confirmed that WPA2-PSK (AES) was enabled to ensure strong encryption for my network. Also replaced the default credentials in use with a strong password via password manager (Bitwarden).

Monitor Network Traffic

Internal network created successfully – Windows and Ubuntu machines are able to communicate.

Launched Wireshark on the Windows VM to sniff packets from the Ubuntu VM across the internal network.

Filtered captured traffic using:

- http – viewed unencrypted web traffic (few generated)

- dns – observed domain name lookups

Suspicious Packets Example (not observed)

- Repeated ping traffic from Ubuntu (this example was observed)
- Traffic destined for unfamiliar IPs
- Example of potential DNS misdirections
- Any other unusual traffic depending on context

Document Findings

Configured basic **Windows Defender Firewall** controls on the Windows VM I set up to enforce traffic control and reduce exposure to unauthorized access to the system.

Accessed the router's administrative interface via the default gateway IP (identified beforehand using ipconfig) to review and update wireless security settings. Confirmed **WPA2-PSK (AES)** was enabled, ensuring a strong encryption standard was in place.

Default Wi-Fi credentials were replaced with a strong, randomly generated password stored securely using **Bitwarden**, reinforcing both password security and future access control.

Created a **VirtualBox** Internal Network environment to connect an Ubunutu and Windows machine together to enable direct communication. Verified connectivy between the systems and initiated live traffic capture (simualting practical packet capture scenarios).

Used **Wireshark** for packet capture on the Windows VM to monitor traffic originating from the Ubuntu VM. Also applied filters to capture **HTTP** and **DNS** traffic specifically, observing key protocol behavior in real time. The visibility into just basic traffic patterns highlighted how much can be observed from packet-level inspection from both offensive (red-team) and defensive (blue-team) objectives.

These foundational security measures can significantly reduce the attack surface by limiting unauthorzied access to systems. Even in simple lab environment, practicing enforcing firewall rules, securing wireless settings, and monitoring traffic tools (such as Wireshark) help simulate the layered defenses needed to detect and prevent threats – and is a great learning experience for anyone interested in information security.

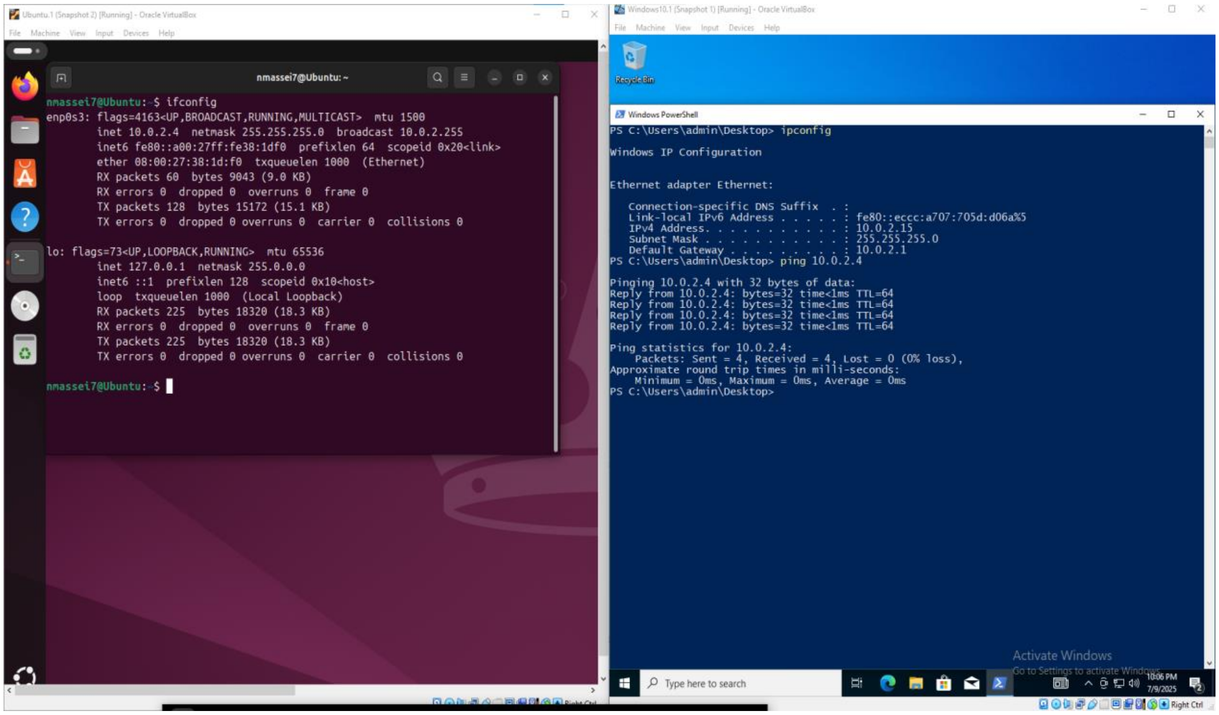
Challenges Faced

While setting up two virtual machines (Windows 10 and Ubuntu), I encountered configuration issues related to internal networking and firewall rule conflicts. Wireshark also initially failed to capture traffic until the correct adapter settings were applied. Troubleshooting these issues deepened my understanding of how VMs are configured.

Reflect on Security Best Practices

Even in larger or more complex environments, the importance of basic security measures really stands out. These small steps I went through like enabling a firewall, using strong passwords, and securing the wireless network create a solid foundation that everything else builds on. While they might seem simple at first, I've come to see how they play a huge role in reducing risk and keeping systems protected. Larger networks obviously need more advanced solutions like intrusion detection systems (IDS), endpoint protection, and network segmentation with VLANs, but the basics still matter just as much.

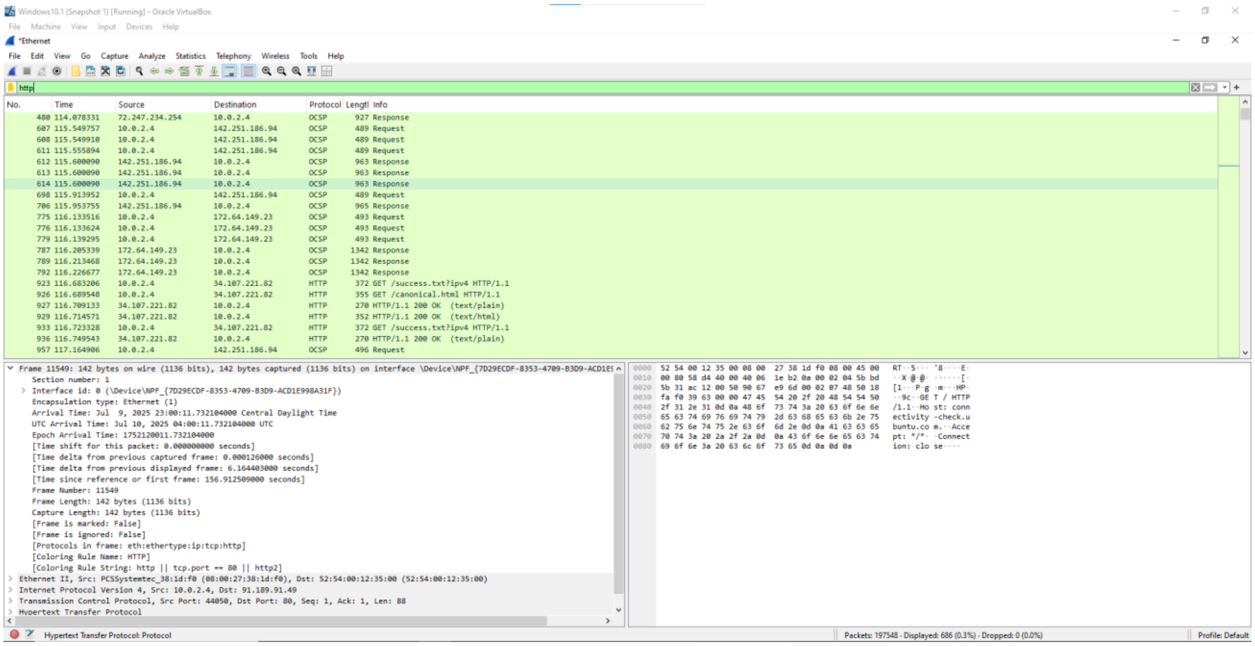
I also think user awareness is key to network security and this really showed in changing default credentials. Things like regular software updates, multi-factor authentication, and avoiding phishing attempts can make a big difference and would be the first things to cover in educating people on the importance of network security. I would also show real-world examples of attacks that happened simply because the basics were ignored as people tend to learn best when they see the actual consequences of oversights like these. Even simple habits, when practiced consistently, can go a long way in strengthening the overall security posture and lowering the attack surface for threat actors.


Ubuntu.1 (Snapshot 2) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
nmassei7@Ubuntu: ~
Windows10.1 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Windows PowerShell
Activate Windows
Go to Settings to activate Windows.
Type here to search
10:06 PM
7/9/2025
Right Ctrl

```
nmassei7@Ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe38:1df0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:38:1d:f0  txqueuelen 1000  (Ethernet)
        RX packets 60  bytes 9043 (9.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 128  bytes 15172 (15.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 225  bytes 18320 (18.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 225  bytes 18320 (18.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

nmassei7@Ubuntu:~$
```

```
PS C:\Users\admin\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::eccc:a707:705d:d06a%5
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1
PS C:\Users\admin\Desktop> ping 10.0.2.4

Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\admin\Desktop>
```

Successful Ping to connected machines


Windows10.1 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Hypertext Transfer Protocol: Protocol
Profile: Default

http

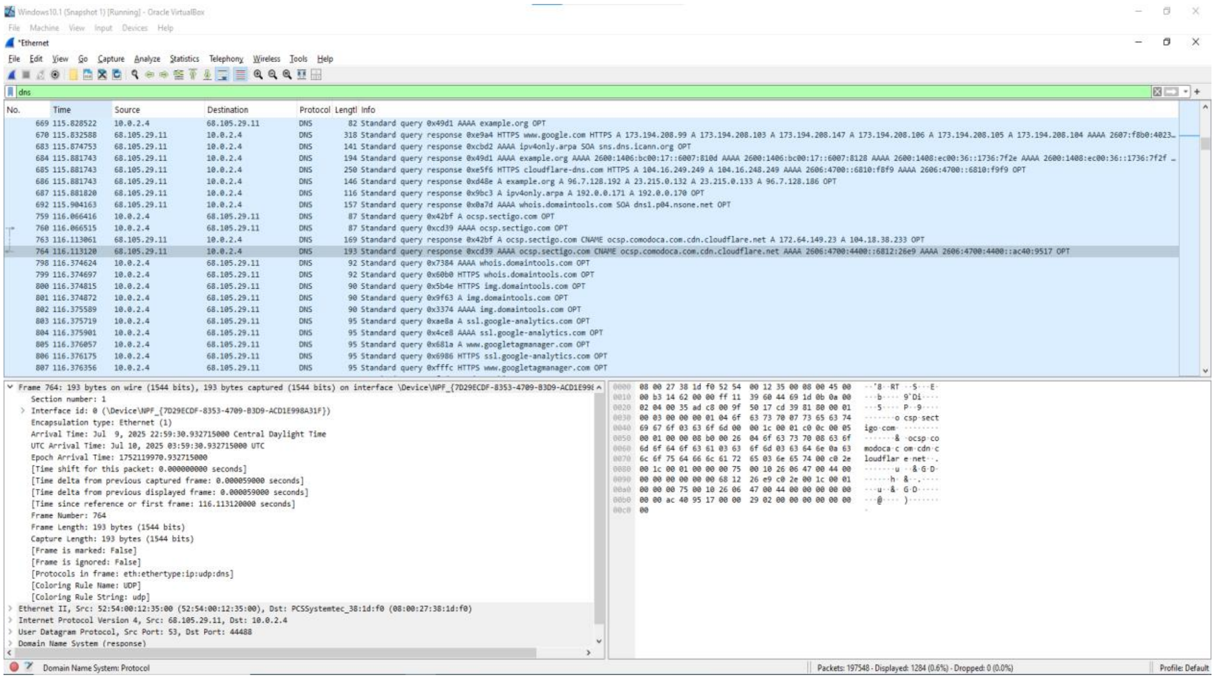
```
No.     Time        Source           Destination      Protocol Lengtl Info
    480 114.078331  72.247.234.254   10.0.2.4         OCSP      927 Response
    607 115.549757  10.0.2.4         142.251.186.94   OCSP      489 Request
    608 115.549910  10.0.2.4         142.251.186.94   OCSP      489 Request
    611 115.555894  10.0.2.4         142.251.186.94   OCSP      489 Request
    612 115.600090  142.251.186.94   10.0.2.4         OCSP      963 Response
    613 115.600090  142.251.186.94   10.0.2.4         OCSP      963 Response
    614 115.600090  142.251.186.94   10.0.2.4         OCSP      963 Response
    698 115.913952  10.0.2.4         142.251.186.94   OCSP      489 Request
    706 115.953755  142.251.186.94   10.0.2.4         OCSP      965 Response
    775 116.133516  10.0.2.4         172.64.149.23    OCSP      493 Request
    776 116.133624  10.0.2.4         172.64.149.23    OCSP      493 Request
    779 116.139295  10.0.2.4         172.64.149.23    OCSP      493 Request
    787 116.205339  172.64.149.23    10.0.2.4         OCSP     1342 Response
    789 116.213468  172.64.149.23    10.0.2.4         OCSP     1342 Response
    792 116.226677  172.64.149.23    10.0.2.4         OCSP     1342 Response
    923 116.683206  10.0.2.4         34.107.221.82    HTTP      372 GET /success.txt?ipv4 HTTP/1.1
    926 116.689548  10.0.2.4         34.107.221.82    HTTP      355 GET /canonical.html HTTP/1.1
    927 116.709133  34.107.221.82    10.0.2.4         HTTP      270 HTTP/1.1 200 OK  (text/plain)
    929 116.714571  34.107.221.82    10.0.2.4         HTTP      352 HTTP/1.1 200 OK  (text/html)
    933 116.723328  10.0.2.4         34.107.221.82    HTTP      372 GET /success.txt?ipv4 HTTP/1.1
    936 116.749543  34.107.221.82    10.0.2.4         HTTP      270 HTTP/1.1 200 OK  (text/plain)
    957 117.164906  10.0.2.4         142.251.186.94   OCSP      496 Request
```

```
v Frame 11549: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{7D29ECDF-8353-4709-B3D9-ACD1E
     Section number: 1
   > Interface id: 0 (\Device\NPF_{7D29ECDF-8353-4709-B3D9-ACD1E998A31F})
     Encapsulation type: Ethernet (1)
     Arrival Time: Jul  9, 2025 23:00:11.732104000 Central Daylight Time
     UTC Arrival Time: Jul 10, 2025 04:00:11.732104000 UTC
     Epoch Arrival Time: 1752120011.732104000
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 0.000126000 seconds]
     [Time delta from previous displayed frame: 6.164403000 seconds]
     [Time since reference or first frame: 156.912509000 seconds]
     Frame Number: 11549
     Frame Length: 142 bytes (1136 bits)
     Capture Length: 142 bytes (1136 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:tcp:http]
     [Coloring Rule Name: HTTP]
     [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: PCSSystemtec_38:1d:f0 (08:00:27:38:1d:f0), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.0.2.4, Dst: 91.189.91.49
> Transmission Control Protocol, Src Port: 44050, Dst Port: 80, Seq: 1, Ack: 1, Len: 88
> Hypertext Transfer Protocol
```

```
0000  52 54 00 12 35 00 08 00  27 38 1d f0 08 00 45 00   RT··5··· '8····E·
0010  00 80 58 d4 40 00 40 06  1e b2 0a 00 02 04 5b bd   ··X·@·@· ······[·
0020  5b 31 ac 12 00 50 90 67  e9 6d 00 02 07 48 50 18   [1···P·g ·m···HP·
0030  fa f0 39 63 00 00 47 45  54 20 2f 20 48 54 54 50   ··9c··GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 63 6f 6e 6e   /1.1··Ho st: conn
0050  65 63 74 69 76 69 74 79  2d 63 68 65 63 6b 2e 75   ectivity -check.u
0060  62 75 6e 74 75 2e 63 6f  6d 2e 0d 0a 41 63 63 65   buntu.co m.··Acce
0070  70 74 3a 20 2a 2f 2a 0d  0a 43 6f 6e 6e 65 63 74   pt: */*· ·Connect
0080  69 6f 6e 3a 20 63 6c 6f  73 65 0d 0a 0d 0a         ion: clo se····
```

Packets: 197548 · Displayed: 686 (0.3%) · Dropped: 0 (0.0%)

http packets captured including multiple “GET” requests and OCSP packets sent over http


Windows10.1 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
```

```
No.   Time        Source        Destination   Protocol Lengtl Info
  669 115.828522  10.0.2.4      68.105.29.11  DNS       82 Standard query 0x49d1 AAAA example.org OPT
  670 115.832588  68.105.29.11  10.0.2.4      DNS      318 Standard query response 0xe9a4 HTTPS www.google.com HTTPS A 173.194.208.99 A 173.194.208.103 A 173.194.208.147 A 173.194.208.106 A 173.194.208.105 A 173.194.208.104 AAAA 2607:f8b0:4023…
  683 115.874753  68.105.29.11  10.0.2.4      DNS      141 Standard query response 0xcbd2 AAAA ipv4only.arpa SOA sns.dns.icann.org OPT
  684 115.881743  68.105.29.11  10.0.2.4      DNS      194 Standard query response 0x49d1 AAAA example.org AAAA 2600:1406:bc00:17::6007:810d AAAA 2600:1406:bc00:17::6007:8128 AAAA 2600:1408:ec00:36::1736:7f2e AAAA 2600:1408:ec00:36::1736:7f2f …
  685 115.881743  68.105.29.11  10.0.2.4      DNS      250 Standard query response 0xe5f6 HTTPS cloudflare-dns.com HTTPS A 104.16.249.249 A 104.16.248.249 AAAA 2606:4700::6810:f8f9 AAAA 2606:4700::6810:f9f9 OPT
  686 115.881743  68.105.29.11  10.0.2.4      DNS      146 Standard query response 0xd48e A example.org A 96.7.128.192 A 23.215.0.132 A 23.215.0.133 A 96.7.128.186 OPT
  687 115.881820  68.105.29.11  10.0.2.4      DNS      116 Standard query response 0x9bc3 A ipv4only.arpa A 192.0.0.171 A 192.0.0.170 OPT
  692 115.904163  68.105.29.11  10.0.2.4      DNS      157 Standard query response 0x0a7d AAAA whois.domaintools.com SOA dns1.p04.nsone.net OPT
  759 116.066416  10.0.2.4      68.105.29.11  DNS       87 Standard query 0x42bf A ocsp.sectigo.com OPT
  760 116.066515  10.0.2.4      68.105.29.11  DNS       87 Standard query 0xcd39 AAAA ocsp.sectigo.com OPT
  763 116.113061  68.105.29.11  10.0.2.4      DNS      169 Standard query response 0x42bf A ocsp.sectigo.com CNAME ocsp.comodoca.com.cdn.cloudflare.net A 172.64.149.23 A 104.18.38.233 OPT
  764 116.113120  68.105.29.11  10.0.2.4      DNS      193 Standard query response 0xcd39 AAAA ocsp.sectigo.com CNAME ocsp.comodoca.com.cdn.cloudflare.net AAAA 2606:4700:4400::6812:26e9 AAAA 2606:4700:4400::ac40:9517 OPT
  798 116.374624  10.0.2.4      68.105.29.11  DNS       92 Standard query 0x7384 AAAA whois.domaintools.com OPT
  799 116.374697  10.0.2.4      68.105.29.11  DNS       92 Standard query 0x60b0 HTTPS whois.domaintools.com OPT
  800 116.374815  10.0.2.4      68.105.29.11  DNS       90 Standard query 0x5b4e HTTPS img.domaintools.com OPT
  801 116.374872  10.0.2.4      68.105.29.11  DNS       90 Standard query 0x9f63 A img.domaintools.com OPT
  802 116.375589  10.0.2.4      68.105.29.11  DNS       90 Standard query 0x3374 AAAA img.domaintools.com OPT
  803 116.375719  10.0.2.4      68.105.29.11  DNS       95 Standard query 0xae8a A ssl.google-analytics.com OPT
  804 116.375901  10.0.2.4      68.105.29.11  DNS       95 Standard query 0x4ce8 AAAA ssl.google-analytics.com OPT
  805 116.376057  10.0.2.4      68.105.29.11  DNS       95 Standard query 0x681a A www.googletagmanager.com OPT
  806 116.376175  10.0.2.4      68.105.29.11  DNS       95 Standard query 0x6986 HTTPS ssl.google-analytics.com OPT
  807 116.376356  10.0.2.4      68.105.29.11  DNS       95 Standard query 0xfffc HTTPS www.googletagmanager.com OPT
```

```
v Frame 764: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface \Device\NPF_{7D29ECDF-8353-4709-83D9-ACD1E99(
    Section number: 1
  > Interface id: 0 (\Device\NPF_{7D29ECDF-8353-4709-B3D9-ACD1E998A31F})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul  9, 2025 22:59:30.932715000 Central Daylight Time
    UTC Arrival Time: Jul 10, 2025 03:59:30.932715000 UTC
    Epoch Arrival Time: 1752119970.932715000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000059000 seconds]
    [Time delta from previous displayed frame: 0.000059000 seconds]
    [Time since reference or first frame: 116.113120000 seconds]
    Frame Number: 764
    Frame Length: 193 bytes (1544 bits)
    Capture Length: 193 bytes (1544 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
> Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSSystemtec_38:1d:f0 (08:00:27:38:1d:f0)
> Internet Protocol Version 4, Src: 68.105.29.11, Dst: 10.0.2.4
> User Datagram Protocol, Src Port: 53, Dst Port: 44488
> Domain Name System (response)
```

```
0000  08 00 27 38 1d f0 52 54  00 12 35 00 08 00 45 00   ··'8··RT ··5···E·
0010  00 b3 14 62 00 00 ff 11  39 60 44 69 1d 0b 0a 00   ···b···· 9`Di····
0020  02 04 00 35 ad c8 00 9f  50 17 cd 39 81 80 00 01   ···5···· P··9····
0030  00 03 00 00 00 01 04 6f  63 73 70 07 73 65 63 74   ·······o csp·sect
0040  69 67 6f 03 63 6f 6d 00  00 1c 00 01 c0 0c 00 05   igo·com· ········
0050  00 01 00 00 08 b0 00 26  04 6f 63 73 70 08 63 6f   ·······& ·ocsp·co
0060  6d 6f 64 6f 63 61 03 63  6f 6d 03 63 64 6e 0a 63   modoca·c om·cdn·c
0070  6c 6f 75 64 66 6c 61 72  65 03 6e 65 74 00 c0 2e   loudflar e·net··.
0080  00 1c 00 01 00 00 00 75  00 10 26 06 47 00 44 00   ·······u ··&·G·D·
0090  00 00 00 00 00 00 68 12  26 e9 c0 2e 00 1c 00 01   ······h· &··.····
00a0  00 00 00 75 00 10 26 06  47 00 44 00 00 00 00 00   ···u··&· G·D·····
00b0  00 00 ac 40 95 17 00 00  29 02 00 00 00 00 00 00   ···@···· )·······
00c0  00                                                 ·
```

Domain Name System: Protocol | Packets: 197548 · Displayed: 1284 (0.6%) · Dropped: 0 (0.0%) | Profile: Default

Captured and observed DNS traffic displaying the records requested during browsing activity.